UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/912,855	07/25/2001	Michael L. Wenocur	A-70557/RMA	6164

7590 03/29/2005

FLEHR HOHBACH TEST ALBRITTON & HERBERT, LLP
Suite 3400
Four Embarcadero Center
San Francisco, CA 94111

EXAMINER	
SHERKAT, AREZOO	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 03/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/912,855	WENOCUR ET AL.	
	Examiner	Art Unit	
	Arezoo Sherkat	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 July 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-40* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-40* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 July 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *01/14/02&2/19/02*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-40 are presented for examination.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-3, 12-13, 19, 23, 25-26, 29-31, and 36-40 are rejected under 35 U.S.C. 102(b) as being anticipated by Davis et al., (U.S. Patent No. 6,064,736 and Davis hereinafter).

Regarding claim 1, Davis discloses a computer program product for use in conjunction with a computer system having a server and a client, the computer program product comprising a computer readable storage medium and a computer program mechanism embedded therein, the computer program mechanism, comprising: a program module that directs the computer system and/or components thereof including at least one or the client or server, to function in a specified manner to provide message communications, the message communications occurring in a computer system hardware architecture neutral and operating system neutral and network transport protocol neutral manner for secure interactive communication sessions, the program module including instructions for:

A. sending to a server, by a client, a first message containing a Client-Nonce, B. receiving said first message including said Client-Nonce by said server, C. sending to the client, by the server in response to said received first message and Client-Nonce, a second message containing a copy of the Client-Nonce extracted from the first message, and a value in the form of a Server-Nonce that was chosen by the Server that is not predictable by the Client and is unlikely to have been previously chosen by the Server, the first message and second message having substantially the same content, format and cryptographic processing (Col. 3, lines 34-67);

D. exchanging third and fourth messages between the client and the server (client to server message) and the server and the client (server to client message) respectively, where the order that said third and fourth messages are sent and received is not material, said third and fourth messages including a content portion that is substantially the same though not necessarily identical and having substantially the same format and cryptographic processing as each other and as with subsequent data transfer messages, the data contents portions of the third and fourth message include a cryptographic transformation of at least the Client-Nonce and Server-Nonce, where the cryptographic transformation is slightly different in the third and fourth messages (Col. 4, lines 1-10 and 42-67 and Col. 6, lines 1-15); and

E. each of the server and client examining the respective received third and fourth messages to confirm that they have the expected contents and thus were created by an entity that knew both the Client-Nonce and the Server-Nonce (Col. 3, lines 34-67 and Col. 4, lines 1-9).

Regarding claim 2, Davis discloses a hardware architecture neutral and operating system neutral and network transport neutral method for secure interactive communication sessions using less software code and network bandwidth than conventional systems, said method comprising:

A. sending to a server, by a client a first message containing a Client-Nonce, B. receiving said first message including said Client-Nonce by said server, C. sending to the client, by the server in response to said received first message and Client-Nonce, a second message containing a copy of the Client-Nonce extracted from the first message, and a value in the form of a Server-Nonce that was chosen by the Server that is not predictable by the Client and is unlikely to have been previously chosen by the Server, the first message and second message having substantially the same content, format and cryptographic processing (Col. 3, lines 34-67);

D. exchanging third and fourth messages between the client and the server (client to server message) and the server and the client (server to client message) respectively, where the order that said third and fourth messages are sent and received is not material, said third and fourth messages including a content portion that is substantially the same though not necessarily identical and having substantially the same format and cryptographic processing as each other and as with subsequent data transfer messages, the data contents portions of the third and fourth message include a cryptographic transformation of at least the Client-Nonce and Server-Nonce, where the cryptographic transformation is slightly different in the third and fourth messages (Col. 4, lines 1-10 and 42-67 and Col. 6, lines 1-15); and

E. each of the server and client examining the respective received third and fourth messages to confirm that they have the expected contents and thus were created by an entity that knew both the Client-Nonce and the Server-Nonce (Col. 3, lines 34-67 and Col. 4, lines 1-9).

Regarding claim 3, Davis discloses further comprising after said sever and said client have examined and confirmed that the third and fourth messages were created by entities that knew both the Client-Nonce and the Server-Nonce (Col. 3, lines 55-67 and Col. 4, lines 1-9); and

F. the Client and Server optionally sending subsequent data messages that have substantially the same format and cryptographic processing as the third and fourth messages (Col. 4, lines 5-10).

Regarding claim 12, Davis discloses wherein the Client-Nonce and Server-Nonce have the same length (Col. 3, lines 34-55).

Regarding claim 13, Davis discloses wherein the Client-Nonce and the Server-Nonce have a length of 8 bytes, 10 bytes, 16 bytes, 20 bytes, 24 bytes, 32 bytes, 64 bytes, 96 bytes, or 128 bytes (Col. 3, lines 34-55).

Regarding claim 19, Davis discloses wherein the Data carried in the first message is a Client-Nonce and the data carried in the second message is the Server-Nonce (Col. 5, lines 55-67 and Col. 6, lines 1-15).

Regarding claim 23, Davis discloses wherein the cryptographic transformation in the third and fourth messages are the same (i.e., the flow of data in both directions between client and server)(Col. 4, lines 2-10).

Regarding claim 25, Davis discloses wherein the cryptographic transformation is a hash of the concatenation of the client-nonce and server-nonce values (Col. 3, lines 55-65).

Regarding claim 26, Davis discloses wherein the hash is selected from the set consisting of MD5, SHA-1, and SHA-256 (Col. 3, lines 55-65).

Regarding claim 29, Davis discloses wherein the third and fourth messages are created using an Encrypted-Data cryptographic primitive, and wherein the Encrypted-Data key for the third message is different than the Encrypted-Data key for the fourth message, and both Encrypted-Data keys are derived from a Master Key that is computed with the aid of one or more applications of a cryptographic hash function applied to at least the Client-Nonce and the Server-Nonce (i.e., SessionKey is encrypted with DES using SecretHash as the DES Key. SecretHash is a function that

performs an MD5 hash of the following: (1) the client nonce exclusive or-ed with the hostname:port of the server; (2) the nonce of the server; and (3) the MD5 hashed password associated to the User Id exclusive or-ed with the hostname:port of the server)(Col. 3, lines 34-67 and Col. 4, lines 1-21).

Regarding claim 30, Davis discloses wherein the Master Key is computed with the aid of one or more applications of a cryptographic hash function applied to the Client-Nonce and the Server-Nonce and to some or all of the information in the previously send or received messages (Col. 3, lines 34-67 and Col. 4, lines 1-21).

Regarding claim 31, Davis discloses wherein the Master Key (MK) is computed as the concatenation of at least a portion of the server-nonce, a portion of the client-nonce, and a portion of the first and second messages (Col. 3, lines 34-67 and Col. 4, lines 1-21).

Regarding claim 36, Davis discloses a method for conducting secure interactive communication sessions between a server and a client, said method comprising:

sending a first message containing a first token chosen by the client, receiving said first message including said first token by the server, sending a second message containing a copy of the first token extracted from the first message, and a second token that was chosen by the server, by the server (Col. 3, lines 34-67);

exchanging third and fourth messages between the client and the server, said third and fourth messages including a content portion having substantially the same format and cryptographic processing as each other, the contents portions of the third and fourth messages including a cryptographic transformation of at least the first token and second token (Col. 4, lines 1-10 and 42-67 and Col. 6, lines 1-15); and

each of the server and client examining the respective received third and fourth messages to confirm that they were created by an entity that knew both the first token and the second token (Col. 3, lines 34-67 and Col. 4, lines 1-9).

Regarding claim 37, Davis discloses wherein the cryptographic transformation is slightly different in the third and fourth messages (i.e., in the first and second message Client-Nonce and Server-Nonce are communicated for two-party authentication and verification purposes, but in third and forth messages the encrypted session using SessionKey is actually established which allows data to flow in both directions between the client and the server over the encrypted session (Col. 4, lines 2-10).

Regarding claim 38, Davis discloses wherein the first token comprises a client-nonce and the second token comprises a server-nonce (i.e., in the first and second message Client-Nonce and Server-Nonce are communicated for two-party authentication and verification purposes)(Col. 3, lines 34-65).

Regarding claim 39, Davis discloses a computer program product for use in conjunction with a computer system having a server and a client, the computer program product comprising a computer readable storage medium and a computer program mechanism embedded therein, the computer program mechanism, comprising: a program module that directs the computer system and/or components thereof including at least one of the client or server, to function in a specified manner to conduct secure interactive communication sessions between a server and a client, the communications occurring in a computer system hardware architecture neutral and operating system neutral and network transport protocol neutral manner for secure interactive communication sessions, the program module including instructions for:

sending a first message containing a first token chosen by the client, receiving the first message including the first token by the server, and sending a second message containing a copy of the first token extracted from the first message, and a second token that was chosen by the server, by the server (Col. 3, lines 34-67);

exchanging third and fourth messages between the client and the server, the third and fourth messages including a content portion having substantially the same format and cryptographic processing as each other, the contents portions of the third and fourth messages including a cryptographic transformation of at least the first token and second token (Col. 4, lines 1-10 and 42-67 and Col. 6, lines 1-15); and

each of the server and client examining the respective received third and fourth messages to confirm that they were created by an entity that knew both the first token and the second token (Col. 3, lines 34-67 and Col. 4, lines 1-9).

Regarding claim 40, Davis discloses wherein the cryptographic transformation is slightly different in the third and fourth messages (i.e., in the first and second message Client-Nonce and Server-Nonce are communicated for two-party authentication and verification purposes, but in third and forth messages the encrypted session using SessionKey is actually established which allows data to flow in both directions between the client and the server over the encrypted session (Col. 4, lines 2-10).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 4-11, 14-15, and 20-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Davis et al., (U.S. Patent No. 6,064,736 and Davis hereinafter), in view of Elgamal et al., (U.S. Patent No. 5,825,890 and Elgamal hereinafter).

Teachings of Davis, with respect to limitations of claims 2 and 3 have been discussed previously.

Regarding claims 4 and 5, Davis does not expressly disclose closing the underlying network connection.

However, Elgamal discloses further comprising after a last message has been communicated between said client and said server or between said server and said client, (G) terminating the session without a separate session termination message by closing the underlying network connection (Col. 15, lines 24-67 and Col. 16, lines 1-51).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Davis by expressly including terminating the session without a separate session termination message by closing the underlying network connection as disclosed by Elgamal. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Elgamal to ensure private communications between application programs running on different computers (Elgamal, Col. 1, lines 1-16).

Regarding claims 6 and 7, Davis does not expressly disclose wherein the underlying network connection is a TCP based connection, by closing the TCP socket.

However, Elgamal discloses wherein the underlying network connection is a TCP based connection, by closing the TCP socket (Col. 5, lines 15-67 and Col. 6, lines 1-35).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Davis by expressly including wherein the underlying network connection is a TCP based connection, by closing the TCP socket as disclosed by Elgamal. This modification would have been obvious

because one of ordinary skill in the art would have been motivated by the suggestion of Elgamal to ensure private communications between application programs running on different computers (Elgamal, Col. 1, lines 1-16).

Regarding claim 8, Davis does not expressly disclose reusing of one or more cryptographic master keys that were established in a previous messaging session.

However, Elgamal discloses wherein the first and second message have no cryptographic processing when the protocol used for the messages is attempting to reuse one or more cryptographic master keys that were established in a previous messaging session, and the first and second messages have substantially the same format, and the Server verifies the existence of a Key-ID from the first message in a server cache of pairs of Key-ID and Master Key values (Col. 9, lines 13-67 and Col. 10, lines 1-23).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Davis by expressly including reuse one or more cryptographic master keys that were established in a previous messaging session, and the first and second messages have substantially the same format, and the Server verifies the existence of a Key-ID from the first message in a server cache of pairs of Key-ID and Master Key values as disclosed by Elgamal. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Elgamal to provide for a secure method of exchanging master key using a public key algorithm and to ensure that security can be

achieved efficiently, with minimal time and effort (Elgamal, Col. 1, lines 40-56 and Col. 7, lines 13-51).

Regarding claim 9, Davis discloses wherein the first message contents containing a Key-ID and a Client-Nonce (i.e., user ID and client-nonce provide ingredients for the server to make up session key)(Col. 4, lines 42-67); and

the second message contents containing the same Key-ID, the same Client-Nonce, and a new Server-Nonce (Col. 3, lines 34-67 and Col. 4, lines 1-9)

Davis does not expressly disclose wherein the first and second messages include fields for Type, Version, and Content-Length.

However, Elgamal discloses wherein the first and second messages include fields for Type, Version, and Content-Length (Col. 21, lines 15-67 and Col. 22, lines 1-67).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Davis by expressly including fields for Type, Version, and Content-Length in the first and second message as disclosed by Elgamal. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Elgamal to provide for a secure method of exchanging master key using a public key algorithm (Elgamal, Col. 7, lines 13-51).

Regarding claim 10, Davis does not expressly disclose wherein the Key-ID is a cryptographic hash of a previously set up Master Key.

However, Elgamal discloses using the previously derived session-identification information, the master key and encryption algorithm (a block cipher plus a hash function)(Col. 8, lines 61-67 and Col. 9, lines 1-56).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Davis by expressly including using the previously derived session-identification information, the master key and encryption algorithm as disclosed by Elgamal. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Elgamal to ensure private communications between application programs running on different computers (Elgamal, Col. 1, lines 1-16).

Regarding claim 11, Davis discloses wherein the cryptographic hash is a MD5 based hash, a SHA-1 based hash, or a SHA-256 based hash (Col. 3, lines 55-65).

Regarding claim 14, Davis does not expressly disclose wherein the first and second messages are cryptographically processed using public key operations.

However, Egamal discloses wherein the first and second messages are cryptographically processed using public key operations and these messages have substantially the same format and cryptographic processing, and the Client and Server

verify the certificate chain in the received second and first message respectively (Col. 6, lines 35-67 and Col. 7, lines 1-51).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Davis by expressly including RSA key exchange algorithm and certificate verification as disclosed by Elgamal. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Elgamal to ensure private communications between application programs running on different computers (Elgamal, Col. 1, lines 1-16).

Regarding claim 15, Davis does not expressly disclose wherein the public key operation comprises an RSA operation or an RSA based operation.

However, Elgamal discloses wherein the public key operation comprises an RSA operation or an RSA based operation (Col. 6, lines 35-67 and Col. 7, lines 1-51).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Davis by including an RSA operation or an RSA based operation as disclosed by Elgamal. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Elgamal to provide for a secure method of exchanging master key using a public key algorithm (Elgamal, Col. 7, lines 13-51).

Regarding claims 20-22, Davis does not expressly disclose wherein the Server need not perform a computationally expense private key operation to initiate a secure session.

However, Elgamal discloses wherein a digitally signed portion of the second message can be pre-computed and/or reused with different messaging sessions, and so that the Server need not perform a computationally expense private key operation to initiate a secure session (i.e., session identification information- master key, cipher block, and hash function- is stored in cache by the client and server applications for a prescribed time intervals)(Col. 8, lines 61-67 and Col. 9, lines 1-56).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Davis by including a digitally signed portion of the second message can be pre-computed and/or reused with different messaging sessions as disclosed by Elgamal. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Elgamal to ensure that security can be achieved efficiently, with minimal time and effort (Elgamal, Col. 1, lines 40-56).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Davis et al., (U.S. Patent No. 6,367,009),

Janson et al., (U.S. Patent No. 5,729,608),

Griffin, (U.S. Publication 2002/0188763),

Diffie et al., (U.S. Patent No. 5,371,794),

VanHeyningen et al., (U.S. Publication No. 2002/0112152),

Ferchichi et al., (U.S. Publication No. 2003/0012382),

Day, (U.S. Patent No. 6,052,784)

Liao et al., (U.S. Patent No. 6,48,405),

Laursen et al., (U.S. Patent No. 6,065,120),

Liao et al., (U.S. Patent No. 6,263,437), and

Arkko et al., (U.S. Publication No. 2002/0052200).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arezoo Sherkat whose telephone number is (571) 272-3796. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

A. Sherkat

Arezoo Sherkat
Patent Examiner
Group 2131
March 4, 2005

ALBERT DECADY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100